ЛИТЕРАТУРА

1. *Hinz S., DuBois P., Stephens J., et al.* MySQL 5.5 Reference Manual [Электронный ресурс]. Режим доступа: http://dev.mysql.com/doc/refman/5.5/en/index.html
2. *Haines R.* The SELinux Notebook — The Foundations. 2nd Edition [Электронный ресурс]. Режим доступа: http://www.freetechbooks.com/efiles/selinuxnotebook/The_SELinux_Notebook_Volume_1_The_Foundations.pdf
3. *Smalley S.* Configuring the SELinux Policy [Электронный ресурс]. Режим доступа: http://www.nsa.gov/research/_files/selinux/papers/policy2.pdf
4. *Loscocco P. A., Smalley S. D.* Meeting Critical Security Objectives with Security-Enhanced Linux [Электронный ресурс]. Режим доступа: http://www.nsa.gov/research/_files/selinux/papers/ottawa01.pdf

УДК 004.94

О МОДЕЛЯХ ЛОГИЧЕСКОГО УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ АТРИБУТОВ

Д. В. Чернов

Доклад посвящен обзору основных работ по моделям логического управления доступом на основе атрибутов, или, иначе, атрибутного управления доступом (Attribute Based Access Control) в компьютерных системах (КС). При таком виде управления доступом предоставление субъекту права доступа к сущности происходит только в том случае, если значения атрибутов субъектов и сущностей позволяют субъекту предоставить данный доступ к сущности. Как правило, атрибутное управление доступом рассматривается как отдельный вид управления доступом наряду с дискреционным, мандатным и ролевым. Вместе с тем КС с управлением доступом на основе атрибутов могут использовать в качестве последних типы, уровни безопасности и роли, включая в себя соответственно отдельные дискреционные, мандатные и ролевые механизмы. В общем случае механизмы функционирования атрибутного управления доступом характерны для систем с мандатным управлением доступом [1].

Атрибутное управление доступом является новым и перспективным видом политик логического управления доступом и информационными потоками в КС. Большинство работ по моделям атрибутного управления доступом (например, [2]) ориентированы на реализацию или оптимизацию подсистемы управления доступом; в них используются оригинальные определения элементов и механизмов защиты, а используемый математический аппарат часто недостаточен для анализа условий нарушения безопасности КС и формального обоснования методов и требований их защиты. В то же время известны модели атрибутного управления доступом, например [3], исследующие вопросы теоретического анализа безопасности.

Исторически первой моделью атрибутного управления доступом может считаться модель типизированной матрицы доступа (ТМД), в которой с каждым объектом системы ассоциирован атрибут-тип. В настоящее время предложено несколько подходов к управлению доступом на основе атрибутов.

В [4] подробно рассматривается модель с динамической ролью. Предполагается, что в системе имеется некоторое количество ролей с заранее определенными правами. К системе имеют доступ неограниченное количество пользователей, которым необходимо приписывать какие-то роли. При этом роли могут меняться с течением времени. Для определения роли пользователя в текущий момент времени используются значе-

ния его атрибутов. В работе рассматривается способ представления механизма с мандатным разграничением доступа с помощью модели с динамической ролью, а также вводится язык, которым можно легко описать правила предоставления ролей.

Работа [2] посвящена рассмотрению вопросов реализации управления доступом для WEB-приложений в сети Интернет. Проводится анализ возможностей, достоинств и недостатков моделей ролевого управления доступом, а также их сравнение с моделями атрибутного управления доступом. Принципиально новым является введение особого типа сущностей, отражающих параметры функционирования КС и учитываемых при проверке прав доступа субъектов к сущностям. С учетом этого формулируется общее определение политики управления доступом на основе атрибутов, предлагается архитектура распределённой системы управления доступом, реализующей политику атрибутного управления доступом.

В работе [3] для анализа безопасности атрибутного управления доступом предлагается использовать атрибутную матрицу доступов (АМД), основанную на моделях Харрисона — Руззо — Ульмана и ТМД. Модель АМД содержит следующие основные изменения:

— с каждой сущностью КС ассоциирован набор атрибутов, принимающих конечное число значений;
— модифицированы операторы создания сущностей и добавлен оператор, меняющий набор значений атрибутов сущностей;
— перед выполнением команды происходит проверка атрибутов фактических параметров-сущностей, и если они не совпадают с указанными в определении команды, то команда не выполняется, кроме того, в условия команды включена проверка истинности предикатов, аргументами которых являются значения атрибутов сущностей.

В работе сформулированы условия, при которых задача проверки безопасности ациклических систем АМД является разрешимой, а также доказана NP-сложность задачи проверки безопасности ациклических систем АМД с конечным множеством значений атрибутов.

Работа [5] представляет новую модель делегирования полномочий, а также её расширение, в которых используются атрибуты делегированного лица. Модели делегирования полномочий строятся для решения проблемы безопасной передачи, или делегирования, полномочий одного пользователя другому. Например, в случае невыхода сотрудника на работу его полномочия, а с ними и определённые права доступа, должны быть распределены между другими сотрудниками. В предыдущих моделях решение о возможности делегирования того или иного полномочия принималось на основе роли или должности, которую имеет делегированное лицо, а также уровня его доступа. Предложенная модель накладывает дополнительные ограничения на выбор делегированного лица, основанные на множестве его атрибутов, таких, как квалификация, опыт работы, должность и т. д. Расширенная модель предоставляет возможность временного делегирования полномочий пользователю, который имеет более низкий уровень доступа. Таким образом, представленные модели являются менее гибкими, но более безопасными, чем предложенные ранее.

В [6] предложен подход к реализации электронной системы сообщений на основе атрибутов. В этой КС формирование списка получателей сообщения, предназначенного для определённой группы пользователей, происходит на основе атрибутов последних. Рассматриваются следующие задачи: минимизация числа получателей сооб-

щения, которым оно не предназначено; отправка конфиденциальных данных в сообщениях только тем пользователям, которые имеют соответствующее право доступа; встраиваемость данного механизма в электронные почтовые системы. Рассматриваются подходы к решению данных задач на основе атрибутного управления доступом и строится архитектура электронной системы сообщений. Приводятся экспериментальные временные данные по формированию списков получателей сообщения прототипом данной системы.

В работе [7] с целью оптимизации применения моделей ролевого управления доступом семейства $RBAC$ рассмотрены методы комбинирования ролевых и атрибутных механизмов. Выделены следующие основные подходы к построению управления доступом:

— использование механизма динамического назначения ролей субъектам в зависимости от значений атрибутов сущностей в некоторый момент времени;
— использование роли как одного из возможных атрибутов субъекта;
— использование атрибутов сущностей в механизме ограничений $RBAC$.

Данный обзор позволяет сформулировать следующие основные свойства атрибутных моделей управления доступом в КС в соответствии с понятиями из [8].

1. В модели имеются множества сущностей E, субъектов $S \subset E$, прав доступа R и объектов-параметров $P = \{p_1, \ldots, p_m\} \subset E$. Каждой сущности поставлено в соответствие некоторое множество атрибутов — переменных с конечными множествами значений, и набор значений атрибутов сущности e обозначен как $A(e)$. Каждой тройке $(s, e, r) \in S \times E \times R$ поставлены в соответствие некоторые параметры $q_1, \ldots, q_k \in P$ и предикат, зависящий от $A(s), A(e), r, A(p_1), \ldots, A(p_k)$, так, что субъект $s \in S$ получает право доступа $r \in R$ к сущности $e \in E$, когда истинен этот предикат. Реализация данного права осуществляется по инициативе субъекта.

2. В момент времени t состояние модели определяется как $G_t = (E_t, V_t, (p_1, A(p_1)), \ldots, (p_m, A(p_m)))$, где E_t — множество сущностей системы в момент времени t и V_t — множество всех реализаций прав доступа (доступов) субъектов к сущностям, которые имеют место в момент времени t. Множество V_t состоит из элементов v_t, где $v_t = ((s, A(s)), (e, A(e)), r)$, $s \in S$, $e \in E$, $r \in R$. Таким образом, состояние КС в модели определяют сущности, текущие реализации прав доступа субъектов к сущностям вместе с их значениями атрибутов и значения атрибутов объектов-параметров. Траекторией функционирования модели называется конечная последовательность состояний $G_0, \ldots, G_T$, где G_0 — начальное состояние, G_i получается из G_{i-1} либо при появлении новой сущности системы, либо при изменении значения атрибута некоторого объекта-параметра, либо при получении субъектом некоторого права доступа к сущности. Множество всех траекторий функционирования КС с начальным состоянием G_0 обозначается $P(G_0)$. Информационные потоки определяются, как в [8].

3. В соответствии с политикой безопасности $P(G_0)$ разбивается на два непересекающихся подмножества: $LP(G_0)$ — разрешённых и $NP(G_0)$ — запрещённых траекторий, и определяются множества $L_a, N_a, L_r, N_r, L_f, N_f$ разрешённых и запрещённых доступов, прав доступа и информационных потоков соответственно. Нарушение безопасности КС определяется как переход в состояние, в котором имеется запрещённый доступ из N_a, или на траектории к которому произошло получение запрещённого права доступа из N_r, или реализован запрещённый информационный поток из множества N_f.

По сравнению с [8], данный механизм определения состояния КС позволяет определить множества L_r, N_r, L_a и N_a не только для КС с дискреционным или ролевым

управлением доступом, в которых, в соответствии с требованиями априорно заданной политики управления доступом, не определены дополнительные ограничения на доступ субъектов к сущностям, но и для некоторых КС с мандатным управлением доступом (например, для политики low-watermark в модели Белла — ЛаПадулы и для политики Type Enforcment) в интерпретации атрибутного управления доступом.

ЛИТЕРАТУРА

1. *Bishop M.* Introduction to Computer Security. USA: Addison-Wesley, 2005.
2. *Yuan E. and Tong J.* Attributed Based Access Control (ABAC) for Web Services // Proc. IEEE Intern. Conf. on Web Services (ICWS'05). Washington, DC, USA, 2005. P. 561–569.
3. *Xinwen Z., Yingjiu L., and Divya N.* An Attribute-Based Access Matrix Model // Proc. ACM Symposium Appl. Computing (SAC'05). Santa Fe, New Mexico, USA, March 2005. P. 359–363.
4. *Al-Kahtani M. A. and Sandhu R.* A model for attribute-based user-role assignment // Annual Computer Security Appl. Conf. Las Vegas, NV, USA. IEEE Computer Society, 2002. P. 353–364.
5. *Chunxiao Y., Zhongfu W., and Yunqing F.* An Attribute-Based Delegation Model and Its Extension // J. Res. Practice Inform. Technol. 2006. V. 38. No. 1. P. 220–234.
6. *Rakesh B., Omid F., Fariba K., et al.* Using Attribute-Based Access Control to Enable Attribute-Based Messaging // Proc. 22nd Annual Computer Security Appl. Conf. (ACSAC'06). Miami Beach, FL, USA, December 2006. P. 403–413.
7. *Kuhn D. R., Coyne E. J., and Weil T. R.* Adding attributes to role-based access control // IEEE Computer. 2010. No. 43(6). P. 79–81.
8. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.